Office de la propriété intellectuelle du Canada

Un organisme d'Industrie Canada

Canadian Intellectual Property Office

An Agency of Industry Canada

Bureau canadien des brevets

Certification

Canadian Patent Office

Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Specification and Drawings, as originally filed, with Application for Patent Serial No: **2,277,633,** on July 19, 1999, by **CERTICOM CORP.,** assignee of Scott A. Vanstone, for "Split-Key Key-Agreement Protocol".

Best Available Copy

Agent certificateur/Certifying Officer

August 23, 2000

Date

Canada

(CIPO 68)

OPIC CIPO

ABSTRACT

This invention relates to a method for generating a shared secret value between entities (E_i) in a data communication system, one or more of the entities having a plurality of members (M_{ij}) for participation in the communication system, each member having a long term private key (P_{rij}) and a corresponding long term public key (P_{Uij}). The method comprises the steps of generating a short term private (x_{ij}) and a corresponding short term public key (X_{ij})for each of the members (M_{ij}); exchanging short term public keys (X_{ij}) of the members within an entity (i). For each member then computing an intra-entity shared key by mathematically combining the short term public keys (X_{ij}) of each the members computing an intra-entity public key (s_i) by mathematically combining its short-term private key (x_{ij}), the long term private key (P_{rij}) and the intra-entity shared key. Next for each entity combining intra-entity public keys (s_i) to derive a group short-term S_i public key; each entity transmitting its intra-entity shared key (X_i) and its group short term public (S_i) key to the other entities; and each entity computing a common shared key K by combining its group short term public key (S_i), with the intra-entity shared key ($\overline{X}_i$), and a group short term public ($\overline{S}_i$) key received from the other entities.

SPLIT-KEY KEY-AGREEMENT PROTOCOL

The present invention relates to the field of key agreement protocols in cryptographic systems.

BACKGROUND OF THE INVENTION

Traditionally, entities communicated on paper and were able to ensure privacy in many ways. With the transition from paper to electronic media however, brings the need for electronic privacy and authenticity. In cryptographic schemes, the entities use primitives, which are mathematical operations together with encoding and formatting techniques to provide security. For each scheme the parties participating in the scheme normally agree upon or exchange certain information before executing the scheme function. The specific information that needs to be agreed upon is detailed for each scheme. Such agreement may be achieved by any means suitable for the application. It may be implicitly built into the system or explicitly achieved by some sort of exchange of information with or without involvement from other parties. In particular, parties often need to agree on parameters and obtain each other's public keys. For proper security, a party needs to be assured of the true owners of the keys and parameters and of their validity. Generation of parameters and keys needs to be performed properly and, in some cases, verification needs to be performed.

In general, the different types of schemes may be defined as follows. Key agreement schemes, in which two parties use their public, private key pairs and possibly other information, to agree on a shared secret key. A signature scheme with appendix is a scheme in which one party signs a message using its private key and any other party can verify the signature by examining the message, the signature, and the signer's cross corresponding public key. In signature schemes with message recovery, one party signs a message using its private key and any other party can verify the signature and recover the message by examining the signature and the signer's corresponding public key. Finally, in encryption schemes, any party can encrypt a message using the recipient's public key and only the recipient can decrypt the message using its corresponding private key.

An example of a key derivation scheme is the MQV (Menezes-Qu-Vanstone). In the MQV scheme, a shared secret value is derived from one party's two key pairs and another

party's two public keys where all the keys have the same discrete log (DL) parameters. In this generalized MQV scheme, it is assumed that the shared secret value is that which is shared between two parties.

However, where each party or entity consists of a collection of parties say $A = \{A_1, A_2 \ldots A_n\}$ and $B = \{B_1, B_2, \ldots B_m\}$ where m is not necessarily equal to n and at least one of m or n is at least two (that is, not both A and B consist of one individual). It is difficult to implement the generalized MQV scheme if these two entities wish to establish a common key in order to communicate privately.

SUMMARY OF THE INVENTION

Accordingly, the present invention seeks to provide a solution to the problem of establishing a common key for private communication between entities wherein the entities include a collection of sub entities.

An advantage of the present invention is that all members of each entity must participate in the scheme and no subcollection of either entity can impersonate its entire entity.

In accordance with this invention there is provided a method for generating a shared secret value between entities in a data communication system, one or more of the entities having a plurality of members for participation in the communication system, each member having a long term private key and a corresponding long term public key, the method comprising the steps of:

(a) generating a short term private and a corresponding short term public key for each of the members;

(b) exchanging short term public keys of the members within an entity;

(c) for each member:

(i) computing an intra-entity shared key by mathematically combining the short term public keys of each said member;

(ii) computing an intra-entity public key by mathematically combining its short-term private key, the long term private key and the first intra-entity key component;

(d) for each entity combining intra-entity public keys to derive a group short-term public key;

(e) each entity transmitting its intra-entity shared key and its group short term public key to the other entities; and

(f) each entity computing a common shared key K by combining its group short term public key, the intra-entity shared key, and the short term public key of the other entities.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

Figure 1 is a schematic diagram of a communication system; and

Figure 2 is a schematic diagram of a protocol according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to figure 1, a schematic diagram of a communication system is shown generally by numeral 10. The system 10 includes a first entity A (12) and a second entity B (14) that exchange data over a communication channel 16. Each of the entities A and B include members A_1, A_2, and B_1, B_2, respectively. It is assumed the entities A and B include processors for performing cryptographic operations and the like. The members A_1, A_2 may for example represent a first group of users on a local area network (LAN) that wish to communicate securely with a second group of users B_1, B_2 on a second LAN or even on the same LAN. In either case the computations may be performed for the entities A (12) and B (14) by for example a LAN server or the like, provided that each member has its own secure boundary.

Accordingly, the present protocol ensures that all members of each entity must participate in the scheme and no sub-collection of either entity can impersonate its entire entity.

Furthermore, it is assumed that each entity and it's associated members A_i, B_i have been initialized with the same system parameters. The system parameters for this protocol are an elliptic curve point P, which is the generating point of an elliptic curve over $F_2{}^m$ of order x. Additionally, each of the members is initialized with respective public and private key pairs.

That is, the members A_i has long term private and public key pairs (a_i, a_iP) and the members B_i have long term private and public key pairs (b_i, b_iP), respectively.

The private key of the entity A is then $(a_1 + a_2)$ and its corresponding public key is $(a_1 + a_2)$ P. Similarly, for entity B its private key is $(b_1 + b_2)$ and its corresponding public key is $(b_1 + b_2)$ P. These public keys are published by the entities.

Now assuming entities A (12) and B (14) wish to agree upon a common key, which may then be used for subsequent cryptographic communications between the activities.

Referring thus to figure 2, a schematic diagram of an embodiment of the protocol according to the present invention is shown generally by numeral 40. The member A_1 generates a random value x_1 (its short term private key, also known as ephemeral or session key) and computes a corresponding value x_1P(its short term public key), similarly, member A_2 generates a random value x_2 and computes a corresponding value x_2P. Preferably $0 < a_i < n-1$ and $0 < x_i < n-1$. Next, the members A_2 and A_1 exchange their session public keys x_1P and x_2P. This may be termed a first intra-entity key exchange.

Next, member A_1 computes $r = x_1P + x_2P$ and similarly, entity A_2 computes $r = x_2P + x_1P$. Thus, establishing an intra-entity shared key.

Next, each member A_1 computes its short term intra-entity public key s_1 using its short term private key and long term private key combined with a function f of the intra-entity public key, that is $s_1 = x_1 + a_1 f(r) \pmod n$, where f is typically a hash function such as SHA-1 and n is the order of the curve. Similarly, member A_2 computes its intra-entity public key $s_2 = x_2 + a_2 f(r) \pmod{n}$.)

The entity A transmits the intra-entity shared key r to the entity B. The entity A also computes an entity or group short term public key, which is derived from a summing of the intra-entity public key of each member $s = s_1 + s_2 = x_1 + x_2 + (a_1 + a_2) f(r) \bmod n$. Entity A then also transmits the group short-term public key s to the entity B.

The entity B similarly computes the analogous information using its own public and private keys using the same computations performed by entity A. Thus, B computes a intra-entity shared key $\bar{r}$ using the short term public keys of each of the members. Next, each of the members in B compute their own intra-entity public key $t_i = y_i + b_i f(\bar{r}) \bmod n$. The entity B then sends $\bar{r}$ to the entity A and computes the group short-term public key $t = t_1 + t_2$ which is transmitted to the entity A.

The entity A then computes a value K which is the shared key between the entities A and B by computing $K = s(\bar{r} + (bP) f(\bar{r})) = s(t)P$. The entity B also computes K using t, r, and aP(or s), $K = t(s)P$.

Consequently, if a member of the entity A, either A_1 or A_2, is not present in the scheme then the group short term public key, s, changes, as does the value for K. Therefore, communication with entity B would not be successful without establishing a new session. Similarly, if either B_1 or B_2 is not present in the scheme then the group short term public key, t, changes, altering the value of K. In this case, communication with A would not be successful without establishing a new session.

Although the above scheme has been described with respect to the elliptic curve systems which is an additive group, it may analogously be used in multiplicative groups. Furthermore the above protocol although exemplified with two members per entity, may be generalized where each party or entity consists of a collection of members say $A = \{A_1, A_2 \ldots A_n\}$ and $B = \{B_1, B_2, \ldots B_m\}$ where m is not necessarily equal to n and at least one of m or n is at least two (that is, not both A and B consist of one individual). The notation may be generalized as follows:

E_i	-	entity i
M_{ij}	-	member j of entity i
Pr_{ij}	-	long term private key of member (ij)
Pu_{ij}	-	long term public key of member (ij)
Pu_i	-	long term public key of entity (i)
x_{ij}	-	short term private key of member (ij)
X_{ij}	-	short term public key of member (ij)
X_i	-	intra-entity shared key of entity i
s_i	-	intra-entity public key of entity i
S_i	-	group or entity short term public key of entity i
$\overline{Pu}_i$	-	long term public key received from the other entities
$\overline{X}_i$	-	intra-entity shared key received from the other entities
$\overline{S}_i$	-	group or entity short term public key received from the other entities

Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for generating a shared secret value between entities (E_i) in a data communication system, one or more of said entities having a plurality of members (M_{ij}) for participation in said communication system, each member having a long term private key (P_{rij}) and a corresponding long term public key (P_{Uij}) said method comprising the steps of:
   (a) generating a short term private (x_{ij}) and a corresponding short term public key (X_{ij})for each of the members (M_{ij});
   (b) exchanging short term public keys (X_{ij}) of the members within an entity (i);
   (c) for each member:
      (i) computing an intra-entity shared key by mathematically combining said short term public keys (X_{ij}) of each said member;
      (ii) computing an intra-entity public key (s_i) by mathematically combining its short-term private key (x_{ij}), the long term private key (P_{rij}) and said intra-entity shared key;
   (d) for each entity combining intra-entity public keys (s_i) to derive a group short-term S_i public key;
   (e) each entity transmitting its intra-entity shared key (X_i) and its group short term public (S_i) key to said other entities; and
   (f) each entity computing a common shared key K by combining its group short term public key (S_i), with the intra-entity shared key ($\bar{X}_i$), and a group short term public ($\bar{S}_i$) key received from the other entities.

2. A method as defined in claim 1, said long term public key being derived from a generator point P and respective ones of said long term private keys.

3. A method as defined in claim 2, said step (a) including each member selecting a random integer x_i and multiplying said point P by a to obtain x_iP, the short term public key.

4. A method as defined in claim 3, said intra-entity-shared key being computed by summing said short term public keys x_iP.

5. A method as defined in claim 4, said intra-entity public key s_i being derived by computing $s_i = x_i + a_i f(\Sigma x_i P)$, where f is a hash function.

6. A method as defined in claim 5, said group short term public key being derived by computing Σs_i.

7. A method as defined in claim 1, said long term public keys (Pu_{ij}) being derived from a generator g and respective ones of said long term private keys (Pr_{ij}).

8. A method as defined in claim 7, said step (a) including the step of each member selecting a random integer (x_{ij}) and exponentiating a function h(g) including said generator to a power $g(x_{ij})$ to obtain the short term public key $X_{ij} = h(g)^{g(xij)}$.

9. A method as defined in claim 8, said intra-entity shared key (X_i) being computed by each entity multiplying each of its short-term public keys X_{ij} together.

10. A method as defined in claim 1, including the step of exchanging long term public key of entity Pu_i between entities.

11. A method as defined in claim 10, each entity computing a common shared key K by combining its group short term public key (S_i), with the intra-entity shared key ($\overline{X}_i$) , and a long term public key of ($\overline{Pu}_i$) received from the other entities.

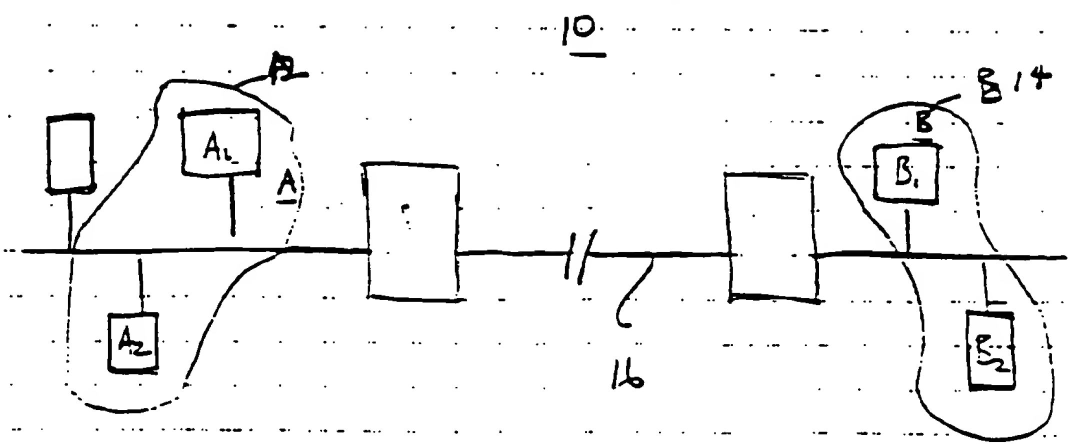

Fig 1

CA 02277633 1999-07-19